NIST Framework for Improving Critical Infrastructure Cybersecurity

Identity-Defined Networking (IDN) helps you significantly reduce cybersecurity risk

As industry's national laboratory, NIST is dedicated to supporting U.S. competitiveness in areas of national importance from communications technology and cybersecurity to advanced manufacturing and disaster resilience. To aid in this process, NIST produces a number of cybersecurity standards, including the Special Publication 800-series and the Cybersecurity Framework.

The Cybersecurity Framework (CSF)

As of May 11, 2017, all federal agencies are now required to adopt the CSF in accordance with Executive Order: *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.*

The CSF offers a set of cybersecurity practices, outcomes, and technical, operational, and managerial security controls that are designed to help organizations manage cybersecurity risk. These controls support the five risk management functions of the CSF: Identify, Protect, Detect, Respond, and Recover. While intended for adoption by the critical infrastructure sector, the foundational set of cybersecurity disciplines that make up the CSF have been supported by government and industry as a recommended baseline for use by any organization, regardless of its sector or size. A recent Gartner report estimated that the CSF is used by approximately 30% of U.S. organizations and projected to reach 50% by 2020.

Identity-Defined Networking enables conformance to the NIST CSF

You can now strengthen your cybersecurity posture by leveraging IDN to build an integrated, automated, simple, and secure network architecture to achieve the security outcomes in the CSF. With built-in security and a level of connectivity that simply hasn't been possible until now, IDN delivers strong cybersecurity risk management practices for each interconnected system to protect the confidentiality, integrity and availability of data.

With Tempered Networks, you can align with the CSF Core and achieve secure connectivity and segmentation at scale for any device, anywhere in the world, across any network environment.

Control Objectives	Tempered Networks
Identify	✓
Protect	✓
Detect	✗
Respond	✓
Recover	✓

 |

Core Function: Identify

Tempered Networks does not provide in-depth asset management; however, no unauthorized devices can connect to the IDN fabric without being whitelisted first via their unique cryptographic identity. This means all connections are authorized, and then documented and reviewed using the Conductor's Visual Trust Map and user activity logs. With simple and secure remote access that can be micro-segmented down to the individual device based on user privilege, managing complex vendor eco-systems is now simple and fast, significantly reducing your supply chain risks.

Core Function: Protect

Establishing and managing identification mechanisms for your network is easy, with access to individual devices within the IDN fabric that is based on machine authentication and authorization of unique cryptographic identities. Through built-in security with peer-to-peer AES 256 encryption and verifiable isolation that ensures data security, you can now significantly reduce the total available attack surface, while at the same time improving availability and resiliency of the network with simple and automated disaster recovery. Achieving the same level of secure connectivity and segmentation with other solutions is simply impractical, if not impossible.

Core Function: Detect

Tempered Networks does not provide any detection capabilities. However, using the RESTful API, you can integrate IDN with other third-party security and networking services like directory services, SIEMs, IPS/IDS, and other monitoring tools. Through simple integration with these detection systems, you can now build event-based logic for real-time isolation, mitigation, and disaster recovery across the adaptive IDN fabric.

Core Function: Respond

IDN helps you respond to security incidents in real-time. Either manually, or using the secure API, you can now remove and quarantine a compromised device out of hundreds of networks—instantly. And for further analysis, suspect traffic can be re-directed and quarantined to a purpose-built lab, without the attacker being aware that the network has changed.

Core Function: Recover

This section is focused on recovery processes, which Tempered Networks does not provide. However, with simple and automated disaster recovery you can achieve a level of availability and resiliency that previously was impractical, if not impossible. This results in significantly reducing the risk of a cyber event, while minimizing interruption of revenue-generating activities.

To learn more about how Tempered Networks can help you comply with NIST CSF security controls, email: info@temperednetworks.com or visit www.temperednetworks.com

 |